King County
Information Technology

Security Guidance While Telecommuting

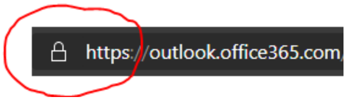
Overview

COVID-19 means many employees are working remotely. KCIT has guidance below on important security to be aware of when working remotely as well as what to do when you need support.

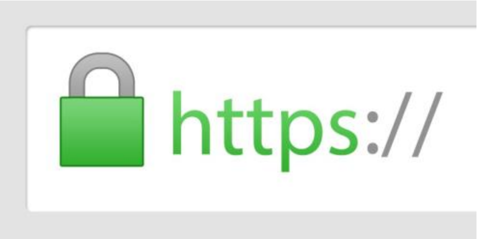
Security Guidance

- Start by watching this video: Create a Cyber Secure Home.
- If possible, use King County laptops, which include County security protections.
- Do not use “open” and unprotected Wi-Fi access points or networks that don’t require a passphrase to connect (referred to as a pre-shared key). To securely set up a home Wi-Fi access point, visit the manufacturer’s website for help. Below are links to some common manufacturers:
    - Netgear
    - Linksys
    - TP-Link
    - D-Link
    - Ubiquiti
    - Cisco

- Use the King County AnyConnect VPN when working with sensitive or regulated data if possible, particularly when using untrusted or public Wi-Fi. Unsure? Check with your supervisor.
- If using public or untrusted Wi-Fi, another good practice while using web browsers is to always use “https” if possible. Look for the "s" in “https” at the beginning of a URL or web address. Also, look for the small padlock symbol that website browsers use to indicate that a secure connection is in place.



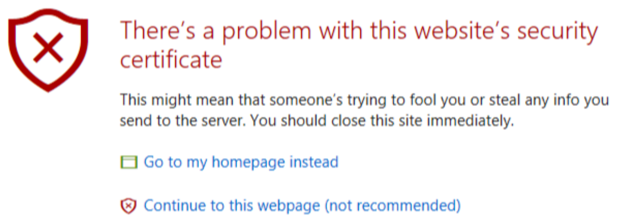
https://outlook.office365.com



https://

- If you see a certificate error, **do not** bypass it, as it is usually an indication of problems or risky websites.

Example of a certificate error:



There's a problem with this website's security certificate

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to my homepage instead

Continue to this webpage (not recommended)

- Use good home office security practices. For example:

  - Family members and friends should not be given access to King County technology or be able to access, view or overhear sensitive or regulated data.
  - Employees should lock or log out of their laptop when stepping away from the device.
  - Report security incidents. This lets the County address the issue quickly. Please do not hesitate to report anything suspicious.

- Home equipment such as Wi-Fi access points should be updated to the latest firmware/software versions and default passwords provided out of the box by the manufacturer should be changed.
- Home software such as web browsers should be updated to the latest versions.
- King County telecommuting policies should be known and followed.

Additional Online Resources

- Home Office Security
- Phone Call Attacks & Scams
- Personalized Scams
- Securing Today's Online Kids

Technical Support for Telecommuters during COVID-19 Response

Employees who need technical assistance equipment should contact the KCIT helpdesk at https://helpdesk.kingcounty.gov/ to live chat with an agent or submit a ticket, or call 206-263-4357 (3-HELP).